# CS3072/CS3605 Final-year Project: Task 1 - Project Synopsis

|  |  |  |  |
| --- | --- | --- | --- |
| **Student** **Number** | 1516552 | **Supervisor** |  |
| **Programme** |  | **Specialism** |  |
| **Provisional Title** |  | | |
| **Problem Definition** | | | |
| Password Manager.  Autofill functionality.  Most websites that uses third-party advertising scripts can use the autofill login details to track the browsing activity of the user. They can run in the background and create fake login/password boxes invisible to the user, which captures the credentials that the password manager then auto-fills. | | | |
| **Aims and Objectives** | | | |
| Aim of this project is to try and achieve a certain level of secure password storage and management withholding the idea of an inevitable vulnerabilities that exists within every security system created.  The use of Random Password Generator each and everytime the login is required.  Focusing on the system as well as the server to efficiently make use of the password manager. i.e. only allowing a Verified Device to be able to login using the random password generator. | | | |
| **Background Sources** | | | |
| <https://www.howtogeek.com/338209/you-should-turn-off-autofill-in-your-password-manager/>   * According to the blog in website, the autofill functionality of the password manager is badly rated. * It highlights the misuse of the integrated autofill functions of browser apps.   <https://crypto.stanford.edu/~dabo/papers/pwdmgrBrowser.pdf> | | | |
| **Approach** | | | |
|  | | | |
| **Evaluation** | | | |
|  | | | |